

UNITED STATES DISTRICT COURT
for the
EASTERN DISTRICT OF WISCONSIN

In the Matter of the Search of

Case Number:

14-m-632

Information associated with email account officealan66@yahoo.com that is stored at premises controlled by Yahoo Inc.

USDC EDWI FILED IN GREEN BAY DIV APR 16 2014 AT _____ O'CLOCK _____ M JON W. SANFILIPPO

APPLICATION & AFFIDAVIT FOR SEARCH WARRANT

I, Matt Schmitz, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

Information associated with email account officealan66@yahoo.com that is stored at premises controlled by Yahoo Inc.

there is now concealed: **Please see attached affidavit, which is hereby incorporated by reference.**

The basis for the search warrant under Fed. R. Crim. P. 41(c) is which is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of a crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Title 18, United States Code, Sections 1343, 1344, 1029, and 1028A.

The application is based on these facts:

- ☒ Continued on the attached sheet, which is incorporated by reference.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me, and signed in my presence.

Date April 16, 2014

City and state: Green Bay, Wisconsin

Applicant's signature
Name and Title: Matt Schmitz, U.S. Postal Inspector

Judge's signature
HONORABLE JAMES R SICKEL
United States Magistrate Court Judge
Name & Title of Judicial Officer

AFFIDAVIT

I, Matthew Schmitz, United States Postal Inspector, being duly sworn, state the following information was developed from the Affiant's personal knowledge and from information furnished to the Affiant by other law enforcement agents and business contacts:

I. INTRODUCTION

1. I have been a Postal Inspector with the United States Postal Inspection Service for approximately ten years and am currently assigned to the Green Bay (WI) Domicile in the Eastern District of Wisconsin. Before becoming a postal inspector I served as a police officer with the Janesville Police Department in Janesville, Wisconsin for one year and as a police officer and detective with the Middleton Police Department in Middleton, Wisconsin for approximately five years. I have knowledge and experience in mail theft, identity theft, forgery, credit card fraud and other property related offenses through training and criminal investigations while employed with the Janesville Police Department, Middleton Police Department, and United States Postal Inspection Service. As a Postal Inspector I am responsible for investigating criminal violations that involve the United States Mail and United States Postal Service. These investigations include, but are not limited to, mail theft, credit card fraud, identity theft, mail fraud, controlled substance distribution, and burglaries and robberies to United States Postal Service facilities. I have conducted identity theft and credit card fraud investigations relating to the theft and/or use of stolen credit card information. I have learned from these investigations that subjects responsible for stealing and/or misusing the personal identifying information of other individuals may retain custody of evidence related to this activity for several weeks or months for future reference or to continue their criminal activity.

PURPOSE

2. I make this affidavit in support of an application for a search warrant on information contained with Yahoo! email account officealan66@yahoo.com. This email address is described herein and in Attachment A, and the information to be seized is described herein and in Attachment B. Information related to this email address is stored at premises owned, maintained, controlled, or operated by Yahoo Inc. located at 701 1st Avenue, Sunnyvale, CA 94089. I have information to

believe that Gregory Looney, Michael E Miller, Christina Bonetti, and unknown persons have participated in a credit card and identity theft scheme through committing acts of wire fraud, bank fraud, access device fraud, and aggravated identity theft in violation of Title 18, United States Code, Sections 1343, 1344, 1029, and 1028A. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this investigation. This affidavit is submitted in support of a search warrant for the message content and data held under email address officealan66@yahoo.com. This email address and the contents contained therein are believed to contain the evidence, fruits and instrumentalities of the foregoing violations. I am requesting authority to search email address officealan66@yahoo.com and seize all items listed in Attachment B as evidence, fruit and instrumentalities of a crime. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Yahoo Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have set forth only the facts that I believe are necessary to establish probable cause to believe that the evidence, fruits, and instrumentalities of the violation of Title 18, United States Code, Sections 1343, 1344, 1029, and 1028A, are presently located at email address officealan66@yahoo.com.

LEGAL BACKGROUND

3. Title 18, United States Code, Section 2703(a) provides, in part:
 - A). A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication that is in electronic storage in an electronic communications system for one hundred and eighty (180) days or less, only

pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days (180) by the means available under subsection (B) of this section.

B). Title 18, United States Code, Section 2703(b) provides, in part:

- 1). A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection
 - a). Without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or Equivalent State warrant.
- 2). Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service –
 - a). On behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and
 - b). Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

C). The government may also obtain records relating to e-mail communications, such as subscriber identifying information, by way of a search warrant. 18 U.S.C. Section 2703(c). No notice to the subscriber is required, 18 U.S.C. Section 2703(c)(2).

PROBABLE CAUSE

4. In or about December, 2013, Appleton (WI) Police Detective Jackie Gleiss contacted me requesting my assistance in a credit card fraud investigation she was working under Appleton Police incident number 13-049078. Detective Gleiss told me the Appleton Police Department had received two credit card fraud complaints from T.L., Wisconsin resident, and L.R., an Ohio resident, that there credit card accounts were charged without their knowledge and permission at Marshalls Steakhouse, 300 W College Ave, Appleton, WI 54911. Detective Gleiss tried to locate the business Marshalls Steakhouse at 300 W College Ave, Appleton, WI 54911, but found no such business existed at this address.
5. In December, 2013, I learned from U.S. Postal Service records that the Appleton (WI) Post Office had received for delivery U.S. Mail addressed to Marshalls Steakhouse at 300 W College Ave., Appleton, WI 54911. Specifically, I learned many of the mail pieces were sent from First Data, a payment processing company headquartered in Atlanta, Georgia. On December 17, 2013, I made contact with First Data employee Arthur Forster regarding the mailings First Data sent to Marshalls Steakhouse in Appleton, WI. Forester told me the First Data account held under the business name Marshalls Steakhouse at 300 W College Ave, Appleton, WI 54911 was associated with credit card fraud and had been closed.
6. On December 18, 2013, I received information from Elavon Special Investigator Deborah Brazie that she learned from Arthur Forster of my inquiring into an account First Data held with Marshalls Steakhouse in Appleton, WI. Investigator Brazie reported that Elavon was also a payment processing company and held accounts with Marshalls Steakhouse (MARR 88 STE RS LLC), Carroll Steak (SC 6 CARR RS LLC), MJ Fox Pub (MT5 FOX RTT LLC), and Richards Steakhouse (G1 Loon Realty LLC). Investigator Brazie reported these four accounts were established in November, 2013 and December, 2013, had mailing addresses in Appleton, WI (Marshalls

Steakhouse, MJ Fox Pub and Richards Steakhouse) and Chippewa Falls, WI (Carroll Steak), and were linked through common phone numbers associated with the accounts. Investigator Brazie reported Elavon closed these accounts in December, 2013 after they began receiving charge disputes (aka chargebacks) from credit holders whose accounts had incurred a charge at Marshalls Steakhouse, MJ Fox Pub, Richards Steakhouse, and Carroll Steak. On April 10, 2014, Investigator Brazie reported Elavon has sustained a monetary loss of approximately \$8,000.00 due to fraudulent credit card transactions held under the business names Marshalls Steakhouse, MJ Fox Pub, Richards Steakhouse, and Carroll Steak. Investigator Brazie also reported Elavon is still receiving chargebacks from credit accounts and, for that reason, she estimated the total loss that Elavon will incur related to the Marshalls Steakhouse, MJ Fox Pub, Richards Steakhouse, and Carroll Steak will be \$54,423.21.

7. During the course of this investigation I reviewed information provided by Elavon on the accounts held under the names Marshalls Steakhouse, MJ Fox Pub, Richards Steakhouse, and Carroll Steak. I saw that the individuals/s who had established these four accounts had directed Elavon to deposit processed credit card transactions into the following bank accounts:
 - a. Marshalls Steakhouse transactions were to be deposited into a BB&T account ending in 6411.
 - b. MJ Fox Pub transactions were to be deposited into a Chase Bank account ending in 1896.
 - c. Richards Steakhouse transactions were to be deposited into a Washington Federal Savings account ending in 0280.
 - d. Carroll Steak transactions were to be deposited into a Bank of America account ending in 6582.
8. During the course of this investigation I received information from BB&T Bank, Washington Federal Savings, and Bank of America regarding the accounts identified above in paragraph 8. I learned from BB&T Bank that the account ending in 6411 was opened in November, 2013 by Michael E Miller of Louisville, KY under the business name MARR 88 STE RS LLC. I learned

from Washington Federal Savings that the account ending in 0280 was opened in November, 2013 by Gregory Looney of Nampa, ID under the business name G1 Loon Realty LLC. I also learned from Bank of America that the account ending in 6582 was opened in November, 2013 by Christina M Bonetti of Port Orchard, WA under the business name SC6 CARR RS LLC.

9. In April, 2014, I received information from Special Agent (SA) Mike Williams of the U.S. Drug Enforcement Agency in Boise, Idaho that he had contacted Idaho resident Gregory Looney related to suspicious money transactions he was associated with. Looney told SA Williams he began working for an individual he knew as "Alan Peters" in or about June, 2013, by incorporating businesses and opening depository bank accounts associated with those businesses. Looney identified one of the companies and bank accounts that he had established as G1 Loon Realty and Washington Federal Savings (account ending in 0280). Looney was then directed by Peters to withdraw cash from these bank accounts and send it, via FedEx, to locations in Massachusetts, Las Vegas, and Ft. Myers, Florida. Looney told SA Williams that the majority of the money he had withdrawn was mailed to "Francis P. Rosen, 13650 Fiddlesticks Blvd #202, Ft. Myers, FL 33912." Looney provided SA Williams with documents showing the amount of money he had mailed to "Francis P. Rosen, 13650 Fiddlesticks Blvd #202, Ft. Myers, FL 33912" totaled approximately \$70,000.00. In April, 2014, I learned through SA Williams and DEA SA Mark Strang that a UPS Store was located at 13650 Fiddlesticks #202 in Ft. Myers, FL. Further, SA Strang told me he had learned from this UPS Store that an individual they knew as "Francis Rosen" had received several mailings at their store and only visited the store when a mailing was available for him. The UPS Store told SA Strang that Rosen provided them with a Massachusetts identification card under ID # S87252951 in the name of "Francis P Rosen, 7 Harriman Court Unit 2, Maynard, MA 01754." This card further identified Rosen as having a date of birth of January 12, 1951. In April, 2014, I queried the CLEAR law enforcement database for information on Francis P Rosen and received information that no one with the name Francis P Rosen having a date of birth of January 12, 1951 or residing at 7 Harriman Court

Unit 2, Maynard, MA 01754 was known to exist. I know from my training and investigative experience in working identity theft and credit card fraud investigations that individuals knowingly involved in schemes that involve credit card fraud and identity theft commonly use fictitious or counterfeit identification in an attempt to conceal their true identities and avoid detection by law enforcement.

10. SA Williams also told me that since approximately May, 2013, Looney has had regular contact with Peters' via through Peters' email addresses of officealan66@yahoo.com and alanpeters686@yahoo.com. I learned from SA Williams that Looney gave SA Williams access to his email account greg@taintedcrown.com for the purpose of reviewing email correspondence Looney had with Peters through email accounts officealan66@yahoo.com and alanpeters686@yahoo.com. SA Williams provided me with documentation showing email correspondence sent from email address alanpeters686@yahoo.com in or about May, 2013, that contained instructions for Looney to complete an employment contract that was attached to the email sent from alanpeters686@yahoo.com. SA Williams also provided me with documentation showing that since approximately June, 2013, email correspondence has been sent from email account officealan66@yahoo.com to Looney's email account with instructions to withdraw money from various bank accounts and send it via overnight FedEx to Francis P. Rosen in Las Vegas, NV, Charleston, South Carolina, Peabody, MA and Fort Myers, Florida. I also saw that in an email sent on August 15, 2013 by officealan66@yahoo.com to greg@taintedcrown.com, the writer, identifying himself as "Joe," provides instructions to Looney on withdrawing money from a bank account, keeping a portion for himself as pay, depositing some into another bank account, and sending the remainder to Michael Miller in Louisville, KY. I saw in much of the email correspondence sent from officealan66@yahoo.com that when Looney was directed to withdraw and mail cash, he was also instructed to wrap the cash in several pieces of paper or envelopes and to make the package look like documents.

11. In my training and experience I have learned that Yahoo Inc. provides a variety of on-line services including electronic mail ("e-mail") access to the general public. Yahoo Inc. allows subscribers to obtain e-mail accounts at the domain name yahoo.com like the e-mail account listed in Attachment A. Subscribers obtain an account by registering with Yahoo Inc. During the registration process, Yahoo Inc. asks subscribers to provide basic personal information. Therefore, the computers of Yahoo Inc. are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Yahoo Inc. subscribers) and information concerning subscribers and their use of Yahoo Inc. services, such as account access information, e-mail transaction information, and account application information.
12. In general, an e-mail that is sent to a Yahoo Inc. subscriber is stored in the subscriber's "mail box" on Yahoo Inc.'s servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Yahoo Inc.'s servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Yahoo Inc.'s servers for a certain period of time.
13. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Yahoo Inc.'s servers, and then transmitted to its end destination. Yahoo Inc. often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Yahoo Inc. server, the e-mail can remain on the system indefinitely. Even if the sender deletes the e-mail, it may continue to be available on Yahoo Inc.'s servers for a certain period of time. A sent or received e-mail typically includes the content of the message, source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message may also be saved by Yahoo Inc. but may not include all of these categories of data.

14. A Yahoo Inc. subscriber can also store files, including e-mails, address books, contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned by Yahoo Inc. Subscribers to Yahoo Inc. might not store on their home computers copies of the e-mails stored in their Yahoo Inc. account. This is particularly true when they access their Yahoo Inc. account through the web, or if they do not wish to maintain particular e-mails or files in their residence.
15. In general, e-mail providers like Yahoo Inc. ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).
16. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Yahoo Inc.'s website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.
17. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints

from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

18. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED


19. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Yahoo Inc., to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

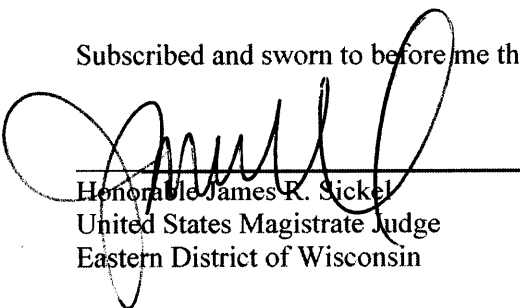
20. Based on the facts set forth in this affidavit, I believe probable cause exists to show that email address officealan66@yahoo.com contains the items listed in ATTACHMENT B of this affidavit. This Court has jurisdiction to issue the requested warrant because it is "a court with jurisdiction over the offense under investigation" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Therefore I am seeking the issuance of a warrant to search the contents and records related to this email account for the items described in ATTACHMENT B, in violation of Title 18, United States Code, Sections 1343, 1344, 1029, and 1028A. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

21. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, e.g., by posting them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.


Matthew B. Schmitz
U.S. Postal Inspector

Subscribed and sworn to before me this 16 day of April, 2014.


Honorable James R. Sickel
United States Magistrate Judge
Eastern District of Wisconsin

ATTACHMENT A: PROPERTY TO BE SEARCHED

This warrant applies to information associated with Yahoo Inc. email account officealan66@yahoo.com that is stored at premises owned, maintained, controlled, or operated by Yahoo Inc. headquartered at 701 1st Avenue, Sunnyvale, CA 94089.

ATTACHMENT B: PARTICULAR THINGS TO BE SEIZED

I. Information to be disclosed by Yahoo Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Yahoo Inc., including any emails, records, files, logs, or information that have been deleted but are still available to Yahoo Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Yahoo Inc. is required to disclose the following information to the government for the account listed in Attachment A:

- a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- d. All records pertaining to communications between Yahoo Inc. and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 1343, 1344, 1029, and 1028A involving the currently unidentified user/s of email account officealan66@yahoo.com since May 1, 2013, including, for the account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Correspondence or information identifying bank accounts, credit card account numbers, personal identifying information of individuals, and the online trading or exchange of bank and credit card account information.
- b. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.
- c. Correspondence or information identifying the names of businesses or LLC's, mailing addresses, and other names and/or email accounts associated with conducting business related to banking, credit transactions, or incorporating businesses.
- d. Records relating to employment offers including advertisements, contracts, and applications.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF
EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Yahoo Inc., and my official title is _____. I am a custodian of records for Yahoo Inc.. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Yahoo Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Yahoo Inc.; and

c. such records were made by Yahoo Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature